What is claimed is:

1. A secure mail proxy system that is provided with a proxy server between a mail server on a LAN (Local Area Network) and the Internet for performing processing that is necessary for managing security such as encryption and attachment of signatures to electronic-mail that is transmitted from said mail server to said Internet and decryption and detection of falsification of encrypted mail with attached signature that has been received from said Internet.

2. A secure mail proxy system according to claim 1 in which a proxy server is arranged between a mail server on a LAN (Local Area Network) and the Internet for carrying out processing relating to security of electronic-mail, said proxy server comprising:

means for encrypting electronic-mail that has been received from said mail server, attaching a signature, and outputting to said Internet; and

means for, when encrypted mail with attached signature that is addressed to said mail server has been transmitted from said Internet, detecting whether or not falsification has occurred in said mail and, if no falsification has occurred, decrypting said encrypted mail and transmitting to said mail server;

said secure mail proxy system being capable of

ensuring the security of electronic-mail on the Internet regardless of the type of mail server, mail client, or user terminal that is used by a user or whether or not security functions are incorporated in the mail server, mail client, or user terminal.

3. A secure mail proxy system according to claim 1 wherein:

a proxy server is arranged between a mail server on a LAN (Local Area Network) and the Internet for carrying out processing relating to security of electronic-mail;

ordinary-text electronic-mail is transmitted from a mail client to said mail server; and

said mail server checks whether or not the destination of said electronic-mail is in said LAN and transmits electronic-mail that has a destination outside said LAN to said proxy server as ordinary text without alteration;

said proxy server comprising:

means for encrypting ordinary-text electronic-mail that has been received from said mail server such that only the mail recipient can decrypt said electronic-mail;

means for attaching a signature of the mail originator to encrypted mail and transmitting the

encrypted electronic-mail with attached signature to said Internet;

means for, in a case in which encrypted electronic-mail with attached signature has been transmitted by way of said Internet addressed to said mail server, checking whether said electronic-mail has been subjected to falsification, and if said electronic-mail has not been subjected to falsification, decrypting and converting said encrypted mail to ordinary-text mail and delivering to said mail server; and

means for, in a case in which said electronic-mail has been subjected to falsification, rejecting the reception of said electronic-mail to prevent the entry of falsified electronic-mail into said LAN;

wherein said mail client requests said mail server for received electronic-mail and obtains ordinary-text electronic-mail from said mail server.

4. A secure mail proxy system according to claim 3 wherein said mail client is either connected directly to said LAN or is connected to said mail server of said LAN by way of at least one of a public line network, a radio-communication network, and a cable television (CATV) network.

5. A secure mail proxy system according to claim

1 that includes: a LAN (Local Area Network); a mail server that is connected to said LAN; and a proxy server provided between said mail server and the Internet for performing processing relating to electronic-mail security;

said proxy server comprising:

a secret key storage means for storing combinations of electronic-mail addresses and secret keys that correspond to these electronic-mail addresses;

a public key storage means for storing combinations of electronic-mail addresses and public keys that correspond to these electronic-mail addresses;

wherein:

said secret keys are used when attaching to electronic-mail the signature of the originator and when decrypting encrypted mail that has been transmitted in addressed to an electronic-mail address in said LAN; and

said public keys are used when encrypting mail such that only the user of the electronic-mail address that is designated in the electronic-mail destination can read the encrypted mail and when checking whether mail has been falsified;

said proxy server being further provided with a data processor that includes:

mail encryption means for obtaining from said public key storage means the public key that corresponds

to the electronic-mail address of the electronic-mail destination and encrypting ordinary-text mail from said mail server using said public key;

mail signature attaching means for obtaining from said secret key storage means the secret key that corresponds to the mail address of the electronic-mail originator, calculating a message digest of said electronic-mail, and, after encrypting the calculated values using said secret key, attaching the encrypted values as the signature of the electronic-mail originator;

mail decryption means for obtaining from said secret key storage means the secret key that corresponds to the electronic-mail address of the electronic-mail destination, and decrypting encrypted mail using said secret key;

mail signature checking means for checking whether or not mail has been falsified by obtaining from said public key storage means the public key that corresponds to the mail address of an electronic-mail originator, decrypting the signature that is attached to mail using said public key; and comparing values of the signature with the message digest of the mail; and

data communication means for receiving ordinary-text electronic-mail from said mail server, transmitting encrypted mail with attached signature that

has been created by said mail encryption means and said mail signature attaching means to said Internet, and further, receiving encrypted mail with attached signature from said Internet and transmitting ordinary-text mail that is obtained by way of said mail signature checking means and said mail decryption means to said mail server.

6. A secure mail proxy system according to claim 5 wherein said mail client is either connected directly to said LAN or is connected to said mail server of said LAN by way of at least one of a public line network, a radio-communication network, and a cable television (CATV) network.

7. A secure mail proxy system according to claim 5 wherein said proxy server is not provided with: a secret key storage means for storing combinations of electronic-mail addresses and secret keys that correspond to the electronic-mail addresses, and a public key storage means for storing combinations of electronic-mail addresses and public keys that correspond to the electronic-mail addresses; but rather:

said secure mail proxy system is provided with: an independent key management server for managing combinations of electronic-mail addresses and secret keys that correspond to the electronic-mail addresses; and an

independent directory server for managing combinations of electronic-mail addresses and public keys that correspond to the electronic-mail addresses;

wherein said mail encryption means, said mail signature attaching means, said mail decryption means, and said mail signature checking means of said proxy server each access said directory server and said key management server and obtain public keys and secret keys.

8. A proxy server that is arranged between a mail server that is connected to a LAN (Local Area Network) and the Internet for performing processing relating to electronic-mail security; is provided with:

a storage device that includes:

a secret key storage section for storing combinations of electronic-mail addresses and secret keys that correspond to the electronic-mail addresses; and

a public key storage section for storing combinations of electronic-mail addresses and public keys that correspond to the electronic-mail addresses;

wherein said secret keys are used when attaching the signature of an originator to electronic-mail and when decrypting encrypted electronic-mail that has been transmitted in to an electronic-mail address in said LAN; and

said public keys are used when encrypting mail

such that only the user of the electronic-mail address that is designated in the electronic-mail destination can read the encrypted mail and when checking whether mail has been falsified;

said proxy server being further provided with a data processor that includes:

mail encryption means for obtaining from said public key storage section the public key that corresponds to the electronic-mail address of the electronic-mail destination and encrypting ordinary-text mail from said mail server using said public key;

mail signature attaching means for obtaining from said secret key storage section the secret key that corresponds to the mail address of an electronic-mail originator, calculating a message digest of said electronic-mail, and, after encrypting the calculated values using said secret key, attaching the encrypted values as the signature of the electronic-mail originator;

mail decryption means for obtaining from said secret key storage section the secret key that corresponds to the electronic-mail address of the electronic-mail destination, and decrypting encrypted mail using said secret key;

mail signature checking means for checking whether or not mail has been falsified by obtaining from

said public key storage section the public key that corresponds to the mail address of an electronic-mail originator, decrypting the signature that is attached to electronic-mail using said public key; and comparing values of the signature with the message digest of the electronic-mail; and

data communication means for receiving ordinary-text electronic-mail from said mail server, transmitting encrypted mail with attached signature that has been created by said mail encryption means and said mail signature attaching means to said Internet, and further, receiving encrypted mail with attached signature from said Internet and transmitting ordinary-text mail that is obtained by way of said mail signature checking means and said mail decryption means to said mail server.

9. A method of managing security of electronic-mail that is transmitted and received between a mail server and the Internet in which a proxy server is provided between a mail server on a LAN (Local Area Network) and the Internet for performing processing relating to electronic-mail security, comprising steps in which:

said proxy server encrypts and attaches a signature to electronic-mail that is to be transmitted to said Internet; and

said proxy server checks for falsification of electronic-mail that is addressed to said mail server from said Internet and decrypts said electronic-mail;

wherein processes necessary for managing security of electronic-mail are performed by said proxy server that is arranged at the point of connection to said Internet;

whereby the security of electronic-mail on the Internet can be ensured regardless of the type of mail server, mail client, or user terminal that is used by the user and regardless of whether the mail server, mail client or user terminal used by the user incorporates security functions.

10. A method of managing security of electronic-mail according to claim 9 wherein a proxy server is arranged between a mail server that is connected to a LAN (Local Area Network) and the Internet; comprising steps in which:

said mail server that has received ordinary-text electronic-mail from a mail client checks whether or not the destination of said electronic-mail is within said LAN and transmits electronic-mail having a destination outside said LAN to said proxy server as ordinary-text without alteration;

said proxy server encrypts ordinary-text

electronic-mail that is sent from said mail server such that only the mail recipient can decrypt said electronic-mail;

the signature of the mail originator is attached and the encrypted electronic-mail with attached signature is transmitted to the Internet;

when encrypted electronic-mail with attached signature has been transmitted in over said Internet addressed to said mail server, said proxy server checks whether or not said electronic-mail has been falsified;

if said electronic-mail has not been falsified, said encrypted electronic-mail is decrypted to ordinary-text mail and then delivered to said mail server;

if said electronic-mail has been falsified, the reception of said electronic-mail is rejected to prevent entry of the falsified electronic-mail into said LAN; and

said mail client is used by the user to request said mail server for received electronic-mail and to receive ordinary-text electronic-mail from said mail server.

11. A method of managing security of electronic-mail according to claim 9, wherein the step in which said proxy server encrypts and attaches a signature to electronic-mail that is to be transmitted to said

Internet includes steps in which:

a user uses a mail client to create electronic-mail and send the electronic-mail to a mail server as ordinary text without alteration;

said mail server checks whether or not the destination of electronic-mail that has been transmitted from said mail client is within the LAN (Local Area Network) to which said mail server is connected;

ordinary-text electronic-mail is delivered to said proxy server when the destination of said electronic-mail is outside said LAN;

said proxy server receives ordinary-text electronic-mail from said mail server, obtains the public key that corresponds to the electronic-mail address of the destination of said electronic-mail from a public key storage section that stores combinations of electronic-mail addresses and corresponding public keys that correspond to electronic-mail addresses, and encrypts said ordinary-text electronic-mail using the public key;

said proxy server obtains the secret key that corresponds to the electronic-mail address of the originator of said electronic-mail from a secret key storage section that stores combinations of electronic-mail addresses and secret keys that correspond to the electronic-mail addresses, calculates a message digest of said electronic-mail, encrypts these calculated values

using the secret key, and attaches these encrypted values to said electronic-mail as the signature of the originator; and

said proxy server sends encrypted mail with attached signature to the Internet.

12. A method of managing security of electronic-mail according to claim 9 wherein the step in which said proxy server checks for falsification of electronic-mail addressed to said mail server from said Internet and decrypts said electronic-mail includes steps in which:

said proxy server receives encrypted electronic-mail with attached signature from said Internet;

said proxy server obtains from said public key storage section the public key that corresponds to the mail address of the electronic-mail originator and decrypts the signature attached to said electronic-mail with said public key;

falsification of said electronic-mail is checked by comparing values of the signature with the message digest of said electronic-mail;

if said electronic-mail has not been falsified, said proxy server obtains from said secret key storage section the secret key that corresponds to the mail address of the destination of said electronic-mail and

decrypts said electronic-mail using said secret key;

electronic-mail that has been decrypted to ordinary text is delivered to said mail server in said LAN;

if said electronic-mail has been falsified, said proxy server rejects the reception of the mail to prevent entry of falsified electronic-mail into said LAN;

said mail server receives ordinary-text electronic-mail from said proxy server; and

the user uses said mail client to request said mail server for mail that has been received and receives ordinary-text mail from said mail server.

13. A recording medium on which is recorded a program for performing processing relating to security of electronic-mail between a mail server that is connected to a LAN (Local Area Network) and the Internet using a proxy server;

wherein a storage device is provided that is in turn provided with:

a secret key storage section for storing combinations of electronic-mail addresses and secret keys that correspond to these electronic-mail addresses, and

a public key storage section for storing combinations of electronic-mail addresses and public keys that correspond to these electronic-mail addresses;

wherein said secret key is used when attaching to electronic-mail the signature of the originator and when decrypting encrypted mail that has been transmitted in to an electronic-mail address in said LAN; and

said public key is used when encrypting electronic-mail such that only the user of the electronic-mail address that is designated in the destination of the electronic-mail can read said electronic-mail and when checking for falsification of electronic-mail;

a program being recorded on said recording medium for causing a computer that constitutes said proxy server to execute the following processes from (a) to (e):

(a) a mail encrypting process in which the public key that corresponds to the electronic-mail address of the destination of electronic-mail is obtained from said public key storage section and ordinary-text mail is encrypted using the public key;

(b) a mail signature attaching process in which the secret key that corresponds to the mail address of the originator of electronic-mail is obtained from said secret key storage section, a message digest of said electronic-mail is calculated; the calculated values are encrypted using the secret key and the encrypted values are attached to electronic-mail as the signature of the

originator;

(c) a mail decryption process in which the secret key that corresponds to the electronic-mail address of the electronic-mail destination is obtained from said secret key storage section and encrypted mail is decrypted using the secret key;

(d) a mail signature checking process in which the public key that corresponds to the mail address of the originator of electronic-mail is obtained from said public key storage section, a signature that is attached to mail is decrypted using the public key, and falsification of mail is checked by comparing values of the signature and the message digest of the mail; and

(e) a data communication process in which ordinary-text mail is received from said mail server, encrypted mail with attached signature is transmitted to the Internet, encrypted mail with attached signature is received from said Internet, and ordinary-text mail is transmitted to said mail server.